



Attorney Docket No. 36321-8006.US01

\$2136

DRW

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant: Schacham, et al.

Serial No.: 09/877,302

Filed: June 8, 2001

Title: **METHOD AND APPARATUS FOR  
BATCHED NETWORK SECURITY  
PROTECTION SERVER PERFORMANCE**

Examiner: Parthasarathy, P.

Group Art Unit: 2136

Confirmation No.: 9725

Attorney Docket No.:  
36321-8006.US01

**CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 1, 2005.

Signed: Maureen Golob  
Maureen Golob

**STATEMENT OF RELATED APPLICATIONS**

**Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450**

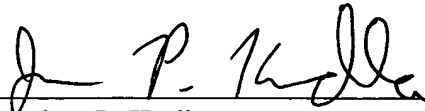
Dear Sir:

Applicant notes for the record that the present patent application is related to U.S. Patent Application No. 09/877,655, entitled "Method and Apparatus for Enhancing Network Security Protection Server Performance", filed on June 8, 2001 (Attorney Docket No. 36321-8007.US01).

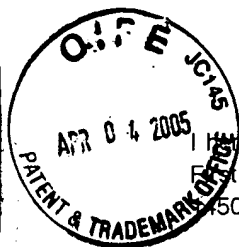
If the Examiner believes that a conference would be of value in expediting the prosecution of this application, he is cordially invited to telephone the undersigned counsel at the number set out below.

Respectfully submitted,  
PERKINS COIE LLP

Dated: April 1, 2005

  
\_\_\_\_\_  
Jonathan P. Kudla  
Reg. No. 47,724

Customer No. 22918  
Perkins Coie LLP  
P.O. Box 2168  
Menlo Park, CA 94026  
Telephone: (650) 838-4300



I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on:

Date: April 1, 2005

By: Maureen Golob  
Maureen Golob

**PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF:

SCHACHAM, ET AL.,

APPLICATION NO.: 09/877,302

FILED: JUNE 8, 2001

FOR: **METHOD AND APPARATUS FOR BATCHED  
NETWORK SECURITY PROTECTION SERVER  
PERFORMANCE**

EXAMINER: PARTHASARATHY,  
P.

ART UNIT: 2136

CONF. NO.: 9725

ATTORNEY DOCKET NO.:  
36321-8006.US01

**Information Disclosure Statement After First Office Action but  
Before Final Action or Notice of Allowance – 37 C.F.R. § 1.97(c)**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

1. Timing of Submission

The information transmitted herewith is being filed *after* three months of the filing date of this application or after the mailing date of the first Office action on the merits, whichever occurred last, but *before* the mailing date of either a final action under 37 C.F.R. § 1.113 or a Notice of Allowance under 37 C.F.R. § 1.311, whichever occurs first. The references listed on the enclosed Form PTO-1449 (modified) may be material to the examination of this application; the Examiner is requested to make them of record in the application.

2. Cited Information

☒ Copies of the following references are enclosed:

- ☒ All cited references  
☐ References marked by asterisks

☐ The following:

04/06/2005 BABRAHA1 00000079 09877302

01 FC:1806

180.00 OP

- ☐ Copies of the following references can be found in parent U.S. Application No. :  
☐ All cited references  
☐ References marked by asterisks  
☐ The following:
- ☐ This application was filed after 30 June 2003 and no copies of U.S. patents nor published applications are enclosed (See Notice of Deputy Commissioner Kunin on 11 July 2003).
- ☐ The following references are not in English. For each such reference, the undersigned has enclosed: (i) a translation of the reference; (ii) a copy of a communication from a foreign patent office or International Searching Authority citing the reference; (iii) a copy of a reference which appears to be an English-language counterpart; or (iv) an English-language abstract for the reference prepared by a third party. Applicant has not verified that the translation, English-language counterpart or third-party abstract is an accurate representation of the teachings of the non-English reference, though, and reserves the right to demonstrate otherwise.
- ☐ All cited references  
☐ References marked by ampersands  
☐ The following:

3. Effect of Information Disclosure Statement (37 C.F.R. § 1.97(h))

This Information Disclosure Statement is not to be construed as a representation that: (i) a search has been made; (ii) additional information material to the examination of this application does not exist; (iii) the information, protocols, results and the like reported by third parties are accurate or enabling; or (iv) the cited information is, or is considered to be, material to patentability. In addition, applicant does not admit that any enclosed item of information constitutes prior art to the subject invention and specifically reserves the right to demonstrate that any such reference is not prior art.

4. Fee Payment (37 C.F.R. § 1.97(c)) or Certification (37 C.F.R. § 1.97(e))

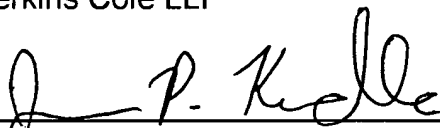
- ☒ Applicant elects to pay the fee under 37 C.F.R. § 1.17(p) - \$180.00.
- ☒ Check enclosed for \$180.00.  
☐ Please charge the above fee(s) to Deposit Account No. 50-2207 this paper is provided in triplicate.

- ☐ Applicant submits that no fee is due in light of the following certification under 37 C.F.R. § 1.97(e) (check only one):
- ☐ In accordance with 37 C.F.R. § 1.97(e)(1), the undersigned hereby states that each item of information submitted herewith was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to this filing of this statement; or
- ☐ In accordance with 37 C.F.R. § 1.97(e)(2), the undersigned hereby states that no item of information submitted herewith was cited in a communication from a foreign patent office in a counterpart foreign application, or, to the knowledge of the person signing the certification after making reasonable inquiry, was known to any individual designated in 37 C.F.R. § 1.56(c), more than three months prior to the filing of this statement.
- ☒ Please charge any underpayment for timely filing of this paper to Deposit Account No. 50-2207.

5. Patent Term Adjustment (37 C.F.R. § 1.704(d))

- ☐ The undersigned states that each item of information submitted herewith was cited in a communication from a foreign patent office in a counterpart application and that this communication was not received by any individual designated in 37 C.F.R. § 1.56(c) more than thirty days prior to the filing of this statement. 37 C.F.R. § 1.704(d).

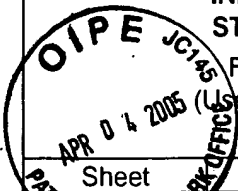
Respectfully submitted,  
Perkins Coie LLP

  
Jonathan P. Kudla  
Registration No. 47,724

Date: April 1, 2005

**Correspondence Address:**

Customer No. 22918  
Perkins Coie LLP  
P.O. Box 2168  
Menlo Park, California 94026  
(650) 838-4300

|  |  |  |  |                          |  |
|--|--|--|--|--------------------------|--|
|  <p><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b></p> <p>Form PTO-1449 (Modified)<br/>(Use several sheets if necessary)</p> |  |  |  | <b>COMPLETE IF KNOWN</b> |  |
|  |  |  |  | Application Number       |  |
|  |  |  |  | Confirmation Number      |  |
|  |  |  |  | Filing Date              |  |
|  |  |  |  | First Named Inventor     |  |
|  |  |  |  | Group Art Unit           |  |
| Examiner Name  |  |  |  | Attorney Docket No.      |  |
| Sheet 1 of 2   |  |  |  |                          |  |

| U.S. PATENT DOCUMENTS |          |                            |                      |  |  |   |
|-----------------------|----------|----------------------------|----------------------|--|--|---|
| Examiner Initials*    | Cite No. | U.S. Patent or Application |                      | Name of Patentee or Inventor of Cited Document | Date of Publication or Filing Date of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
|                       |          | NUMBER                     | Kind Code (if known) |  |  |   |
|                       |          |                            |                      |  |  |   |
|                       |          |                            |                      |  |  |   |

| FOREIGN PATENT DOCUMENTS |          |                               |          |                      |   |  |   |   |
|--------------------------|----------|-------------------------------|----------|----------------------|---|--|---|---|
| Examiner Initials*       | Cite No. | Foreign Patent or Application |          |                      | Name of Patentee or Applicant of Cited Document | Date of Publication or Filing Date of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear | T |
|                          |          | Office                        | NUMBER   | Kind Code (if known) |   |  |   |   |
|                          | 1.       | WO                            | 01/03398 |                      | IBM Corp and IBM UK Limited                     | 01/11/2001   |   |   |
|                          |          |                               |          |                      |   |  |   |   |
|                          |          |                               |          |                      |   |  |   |   |
|                          |          |                               |          |                      |   |  |   |   |
|                          |          |                               |          |                      |   |  |   |   |

| OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS |          |   |  |   |
|---|----------|---|--|---|
| Examiner Initials*                              | Cite No. | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published. |  | T |
|   | 2.       | Netscape; "Netscape Proxy Server Administrator's Guide, Version 3.5 for Unix"; February 25, 1998; Retrieved from the Internet.  |  |   |
|   | 3.       | "PKCS #1 v2.0 Amendment 1: Multi-Prime RSA," 2000   |  |   |
|   | 4.       | "Security Protocols Overview (An RSA Data Security Brief)", RSA Data Security, 1999, <a href="http://www.comms.scitech.susx.ac.uk/fft/crypto/security_protocols.pdf">http://www.comms.scitech.susx.ac.uk/fft/crypto/security_protocols.pdf</a> , pages 1-4.     |  |   |
|   | 5.       | Boneh, D., "Twenty Years of Attacks on the RSA Cyrptosystem," Notices of the AMS, Vol 46, No. 2, pp. 203-213, 1999  |  |   |
|   | 6.       | Boneh, et al., "An Attack on RSA Given a Small Fraction of the Private Key Bits," ASIACRYPT '98, LNCS 1514, pp. 25-34, 1998   |  |   |
|   | 7.       | Boneh, et al., "Cryptanalysis of RSA with Private Key $d$ Less than $N^{0.292}$ ," (extended abstract), 1999  |  |   |

|  |                 |
|--|-----------------|
| EXAMINER   | DATE CONSIDERED |
| <p><small>*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).</small></p> |                 |

|   |                   |    |   |                          |               |  |
|---|-------------------|----|---|--------------------------|---------------|--|
| <b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br>Form PTO-1449 (Modified)<br>(Use several sheets if necessary) |                   |    |   | <b>COMPLETE IF KNOWN</b> |               |  |
|   |                   |    |   | Application Number       | 09/877,302    |  |
|   |                   |    |   | Confirmation Number      | 9725          |  |
|   |                   |    |   | Filing Date              | June 8, 2001  |  |
|   |                   |    |   | First Named Inventor     | Hovav SHACHAM |  |
|   |                   |    |   | Group Art Unit           | 2136          |  |
| Examiner Name   | PARTHASARATHY, P. |    |   |                          |               |  |
| Attorney Docket No.   | 36321-8006.US01   |    |   |                          |               |  |
| Sheet   | 2                 | of | 2 |                          |               |  |

| OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS |          |   |   |
|---|----------|---|---|
| Examiner Initials*                              | Cite No. | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published. | T |
|   | 8.       | Boneh, et al., "Efficient Generation of Shared RSA Keys," (extended abstract)   |   |
|   | 9.       | Durfee, G., et al., "Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacypt '99," ASIACRYPT 2000, LNCS 1976, pp. 14-29, 2000   |   |
|   | 10.      | Fiat, A. "Batch RSA," Springer-Verlag, 1998   |   |
|   | 11.      | Großschädl, J., et al., "The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip," 2000   |   |
|   | 12.      | Immerman, N., "Homework 4 with Extensive Hints," 2000   |   |
|   | 13.      | Menezes, A., et al., "Handbook of Applied Cryptography," 1996 CRC Press, pp. §8.2-8.3 and §14.5   |   |
|   | 14.      | Oppliger, R.; "Authorization Methods for E-Commerce Applications"; 1999   |   |
|   | 15.      | Shacham, H., et al., "Improving SSL Handsake Performance via Batching," Topics in Cryptology, pp. 28-43, 2001   |   |
|   | 16.      | Shand, M., et al., "Fast Implementations of RSA Cryptography," 1993   |   |
|   | 17.      | Sherif, M.H., et al., "SET and SSL: Electronic Payments on the Internet," IEEE, pp. 353-358 (1998)  |   |
|   | 18.      | Stallings, W., "IP Security," Network Security Essentials, Applications and Standards, Chapters 6 and 7, pp. 162-223, 2000  |   |
|   | 19.      | Takagi, T., "Fast RSA-Type Cryptosystem Modulo $p^kq$ ," 1998   |   |
|   | 20.      | Takagi, T., "Fast RSA-Type Cryptosystems Using N-Adic Expansion," Advances in Technology – CRYPTO '97, LNCS 1294, pp. 372-384, 1997   |   |
|   | 21.      | Wiener, M., "Cryptanalysis of Short RSA Secret Exponents," 1989   |   |

|  |                 |
|--|-----------------|
| EXAMINER   | DATE CONSIDERED |
| *EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s). |                 |